Published: 11/05/2021
Creator: Liljana Vall
Approver: Stefan Albertsson
Security class: Public-external use

Document No: GUI-15363
Version: 1
Next review: 11/05/2022

Whistleblowing Guideline

At AddSecure, we're committed to acting with integrity. In line with our Code of Conduct we commit to comply with the rules and regulations of each country in which we operate, and we do not accept any form of corruption or discrimination. We take personal responsibility and speak up.

Background and purpose

AddSecure strives to achieve transparency and a high level of business ethics. Our whistleblowing service offers a possibility to alert us about suspicions of misconduct in confidence. It is an important tool for reducing risks and maintaining trust in our operations by enabling us to detect and act on possible misconduct at an early stage.

Guideline statement

Whistleblowing can be done by any person openly or anonymously.

This guideline is based on the EU General Data Protection Regulation, EU Directive on whistleblower protection and national legislation on whistleblowing.

When to blow the whistle

The whistleblowing service can be used to alert us about serious risks affecting individuals, our company, the society or the environment.

The processing may only refer to data about serious improprieties concerning:

- accounting, internal accounting controls, auditing matters, fight against bribery, banking- and financial crime, or
- other serious improprieties concerning the company's or the group's vital interests or the life or health of individual persons, as for instance serious environmental crimes, major deficiencies that regard the security at the place of work and very serious forms of discrimination or harassments.

Employees are asked to contact their supervisor or manager for issues relating to dissatisfaction in the workplace or related matters, as these issues cannot be investigated in the scope of the whistleblowing.

Published: 11/05/2021
Creator: Liljana Vall
Approver: Stefan Albertsson
Security class: Public-external use

Document No: GUI-15363
Version: 1
Next review: 11/05/2022

A person who blows the whistle does not need to have firm evidence for expressing a suspicion. However, deliberate reporting of false or malicious information is forbidden. Abuse of the whistleblowing service is a serious disciplinary offence.

Please note there could be restrictions on the use of a whistleblowing service in certain countries.

How to blow the whistle

There are different ways to raise a concern:

1. Contact a supervisor or manager within our organization.
2. Contact Chief People & Culture Officer
3. Post an anonymous or confidential message through the whistleblower communication channel to the whistleblowing team: https://report.whistleb.com/addsecure

We encourage anybody who shares their suspicions to be open with their identity. All messages received will be handled confidentially. For those wishing to remain anonymous, we offer a channel for anonymous reporting. The whistleblowing channel enabling anonymous messaging is administrated by WhistleB, an external service provider. All messages are encrypted. To ensure the anonymity of the person sending a message, WhistleB deletes all meta data, including IP addresses. The person sending the message also remains anonymous in the subsequent dialogue with responsible receivers of report.

The investigation process

The whistleblowing team

Access to messages received through our whistleblowing channel is restricted to appointed individuals with the authority to handle whistleblowing cases. Their actions are logged, and handling is confidential. When needed, individuals who can add expertise may be included in the investigation process. These people can access relevant data and are also bound to confidentiality.

If a person raises a concern directly to a supervisor, manager or by contacting the whistleblowing team in person the message is treated according to these guidelines.

Receiving a message

Upon receiving a message, the whistleblowing team decides whether to accept or decline the message. If the message is accepted, appropriate measures for investigation will be taken (please see Investigation below).

The whistleblowing team may decline to accept a message if:

- the alleged conduct is not reportable conduct under this Whistleblowing guideline
- the message has not been made in good faith or is malicious
- there is insufficient information to allow for further investigation
- the subject of the message has already been solved

If a message includes issues not covered by the scope of this Whistleblowing guideline, the whistleblowing team should take appropriate actions to get the issue solved.

The whistleblowing team will send appropriate feedback within 3 (or maximum 6 months) upon the date of receiving the report.

Whistleblowers are urged to not include sensitive personal information about anybody mentioned in a message if it is not necessary for describing the concern.

Investigation

All messages are treated seriously and in accordance with this Whistleblowing guideline. No one from the whistleblowing team, or anyone taking part in the investigation process, will attempt to identify the whistleblower.

- The whistleblowing team can, when needed, submit follow-up questions via the channel for anonymous communication.
- A message will not be investigated by anyone who may be involved with or connected to the misgiving.
- The whistleblowing team decides if and how a whistleblowing message should be escalated.
- Whistleblowing messages are handled confidentially by the parties involved.

Whistleblower protection in the case of non-anonymous whistleblowing

A person expressing genuine suspicion or misgiving according to these guidelines will not be at risk of losing their job or suffering any form sanctions or personal disadvantages as a result. It does not matter if the whistleblower is mistaken, provided that he or she is acting in good faith.

Subject to considerations of the privacy of those against whom allegations have been made, and any other issues of confidentiality, a non-anonymous whistleblower will be kept informed of the outcomes of the investigation into the allegations.

In cases of alleged criminal offences, the whistleblower will be informed that his/her identity may need to be disclosed during judicial proceedings.

Protection of, and information to, a person specified in a whistleblower message

The rights of the individuals submitting the message or specified in a whistleblower message are subject to the relevant data protection laws. Those affected will be entitled to the right to access data relating to themselves and should the information be incorrect, incomplete or out of date to require amendments or deletion of data.

These rights are subject to any overriding safeguarding measures required to prevent the destruction of evidence or other obstructions to the processing and investigation of the case.

Deletion of data

Personal data included in a whistleblowing messages and investigation documentation is deleted when the investigation is complete, with the exception of when personal data must be maintained according to other applicable laws. Permanent deletion is carried out 30 days after completion of the investigation. Investigation documentation and whistleblower messages that are archived should be anonymised under GDPR; they should not include personal data through which persons can be directly or indirectly identified.

Transfer of data outside the EEA

Data is stored within the EU. There is a general prohibition on the transfer of personal data out of the European Economic Area (EEA) unless specific mechanisms are used to protect data.

NB. The scope of this Whistleblowing guideline does not include potential transfer of personal data from the EEA to affiliates located outside the EEA.

Audience

This guideline applies to everyone working at AddSecure, whether as an employee, consultant, board member or part of the group management.

Roles and responsibilities

The Chief Executive Officer (CEO), Stefan Albertsson, is responsible for ensuring compliance with this Guideline.

The Chief People & Culture Officer (CP&CO), Liljana Vall, is the owner of this guideline and is responsible for coordinating, driving implementation and for reporting on progress.

Published: 11/05/2021
Creator: Liljana Vall
Approver: Stefan Albertsson
Security class: Public-external use

Document No: GUI-15363
Version: 1
Next review: 11/05/2022

Each Chief of Group Function and Business Unit President is responsible for ensuring that activities carried out and instructions adopted are in accordance with this Guideline.

Exceptions

Any need for exceptions to this guideline must be clearly defined and documented. All exceptions shall be approved by the authorized approver.

Monitoring of compliance

- This guideline is annually approved by the CEO, following a review by the guideline owner for content and correctness.
- The guideline owner annually reports on guideline compliance to the CEO or directly to the Board.

References

- Code of Conduct
- Business Partner Code of Conduct
- People & Culture Policy